PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32 | A1

(11) International Publication Number: WO 98/24206

(43) International Publication Date: 4 June 1998 (04.06.98)

(21) International Application Number: PCT/US97/21789

(22) International Filing Date: 21 November 1997 (21.11.97)

(30) Priority Data:
08/757,838 27 November 1996 (27.11.96) US

(71) Applicant: ESCO ELECTRONICS CORPORATION [US/US]; Suite 200, 8888 Ladue Road, St. Louis, MO 63124 (US).

(72) Inventors: WOOTTON, John, R.; 700 Rugby Court, St. Louis, MO 63141 (US). WALDMAN, Gary, S.; 12934 Walnut Way, St. Louis, MO 63146 (US). HOBSON, Gregory, L.; 17 Upper Dardenne Farms Drive, St. Charles, MO 63304 (US).

(74) Agent: MULLER, J., Joseph; Polster, Lieder, Woodruff & Lucchesi, 763 South New Ballas Road, St. Louis, MO 63141 (US).

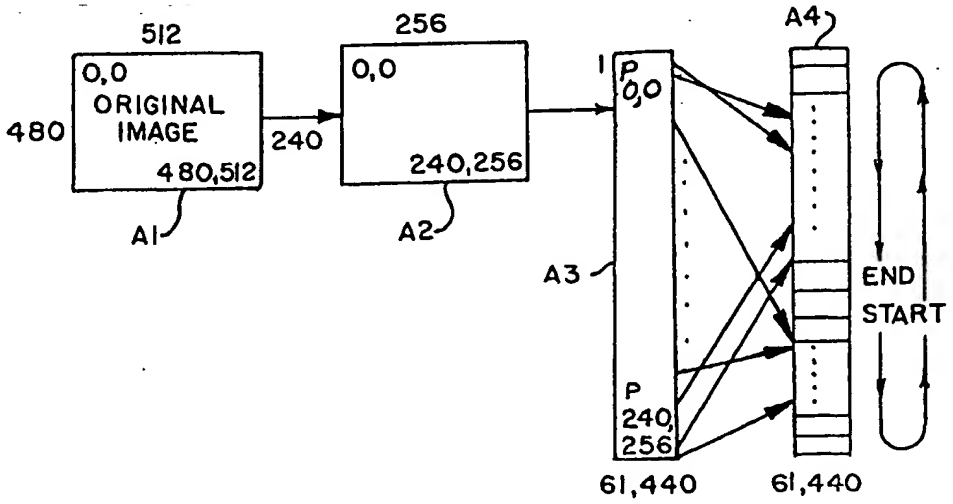
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: AUTHENTICATION ALGORITHMS FOR VIDEO IMAGES



(57) Abstract

A method of authenticating a video image created by a camera (V) or similar video device. The image is formed into a first 2-dimensional pixel array (A1) with each pixel ($P_{m,n}$) represented by a data word of a predetermined length. This formatted array is converted into a second 2-dimensional array (A2) which may be made smaller than the first array by eliminating rows and columns from the formatted array. A first linear vector (A3) is created using the data words in the second array, and a second linear vector (A4) is created by repositioning the data words from the first linear vector in a random pattern. A checksum is created by summing the contents of all of the data words in the second linear vector beginning at a location established by a pre-established formula. A header (H) is formed using the resulting checksum, information identifying the device used to create the image, and the time the image is formed. The header is attached to the formatted image and is transmitted and stored with the formatted image to subsequently authenticate the contents of the original image.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

AUTHENTICATION ALGORITHMS FOR VIDEO IMAGES

Technical Field

This invention relates to the authentication of visual images such as are produced by a video camera or the like, and more particularly to a method of authentication employing algorithms to encode information by which the image can be authenticated.

Background Art

There are a variety of situations in which it is important to know that a visual image such as an image transmitted from one location to another, or a stored image which is to be used at a later time is provided or maintained in the exact form in which it was produced. In the medical field, for example, it is now commonplace to transmit a picture (a visual image) of a patient from one site (a local hospital, for example) to another (the location of a specialist). The image may be an x-ray, CAT scan image, or other image of the patient. Because the image may be used in making a diagnosis, describing a medication or course of treatment, or viewed by a specialist while surgery is being performed, any inaccuracies in the received image can potentially have serious consequences. And, it is known that transmission errors due to noise on the transmission line, temporary disruptions, etc. do occur.

As a further example, many police interrogation rooms are equipped with video equipment so the police examination of a suspect can be recorded. The resulting record can then be used for evidentiary purposes, as well as to defend the police against charges by a suspect that he was mistreated or that a confession was forced from him.

In security systems, to use another example, a video system may capture the image of an intruder during an unauthorized entry. The image therefore can become part of the evidence which is used to prosecute a suspect. To use the image as evidence against the suspect at trial, it is necessary to maintain the image in its original form and do so in a way that the custodian of the evidence can

clearly demonstrate to a court that the image has not been tampered with. It is well known that technology exists by which images can be modified. Such technology can be used to alter the image in such a way that its evidentiary value is destroyed. It is thus important to provide a foolproof method by which tampering can be prevented, or if tampering occurs, it is readily discernible.

Disclosure of the Invention

Among the several objects of the present invention may be noted the provision of a method of authenticating visual images so to prevent tampering with the image, or if the image is transmitted from one location to another, to make it easy to determine if the image which was received exactly corresponds with that which was transmitted;

the provision of such an authentication method in which data representing the content of the whole or a portion of the image is encrypted at the time the image is produced with this encrypted portion of the image being maintained with the entire image for subsequent authentication of the image;

the provision of such a method in which the encryption of the portion of the image is accomplished using an algorithm that has as a factor elements of the time at which the image is produced, these elements including the month, day, hour, and minute at which the image is produced;

the provision of such a method in which the image content encryption code changes minute by minute, so the results from the encryption of an image at one minute produces an authentication code which is different from the authentication code which would result if the encryption were made a minute earlier or a minute later;

the provision of such a method by which, once the image is authenticated, if the image subsequently tampered with, or otherwise altered, such tampering or alteration is not only immediately discernible, but the portion of the image which has been tampered with or altered can be readily identified;

the provision of such a method by which the visual image is converted to a data format arranged in a first array and subsequently processed through successive arrays or linear vectors as part of the encryption process;

the provision of such a method in which a checksum value is ultimately derived for the processed image, the checksum value then being placed in a header attached to the original image, the image and header then being stored or transmitted together so the checksum information can be used to provide image authentication;

the provision of such a method to further include in the header information as to where the image was taken and the time at which the image was formed;

the provision of such a method in which encryption codes used in the algorithm used can be varied from one location to another, and in which the codes are periodically changed;

the provision of such a method which is useful, for example, in transmitting pictorial medical information from one location to another to verify that an image which is received corresponds with that transmitted, or in a security system for monitoring a facility and detecting a breach in security at the facility, especially where evidence of the breach is captured by a camera and it is important to subsequently authenticate the image produced for use by law enforcement officials, or in court; and,

the provision of such a method in which the algorithm used for producing the authentication is readily incorporated in image processing equipment located at the site where images are produced so authentication for the image can be created when the image is produced.

In accordance with the invention, generally stated, a method is taught for authenticating a video image created by a camera or other video device. The visual image is transformed into a data format with a 2-dimensional array being created in which each pixel forming the image is represented by a data word of predetermined length. This array may be converted into a second 2-dimensional array of a size different than that of the first array to reduce the required data

transmission rate. This is not an essential part of the algorithm but may simply be a practical necessity. It will be understood that the algorithm works for all pixel formats (512x480, 384x288, etc.). This conversion is performed using a set of rules by which certain rows and columns in the formatted array are eliminated. A first linear vector is now formed and includes the data words transferred from the first to the second 2-dimensional array. A second linear vector is formed by rearranging the data words in the first linear vector, the new locations of the data words in the second linear vector being randomly selected. A checksum is determined using the data words as arranged in the second linear vector. A header is created using the resulting checksum, information identifying the device used to create the visual image, and the time the visual image is produced. This header is attached to the formatted array. Other objects and features will be in part apparent and in part pointed out hereinafter.

Brief Description of Drawings

In the drawings, Fig. 1 represents a facility where a security system utilizing the image encoding and authentication method of the present invention is installed as an example of the usefulness of the method;

Fig. 2 is a simplified block diagram of an image processing system in which the authentication process is employed;

Fig. 3 is a representation of the steps performed in accordance with the method to produce an image authentication;

Fig. 4 illustrates a 2-dimensional arrangement of data words representing pixels forming the visual image;

Fig. 5 illustrates a linear vector formed by converting a 2-dimensional array;

Fig. 6 illustrates a portion of the process by which a checksum is produced for image authentication;

Fig. 7 is a simplified representation of a header which is created using the checksum and information relating to the time and place the image was produced;

Fig. 8 is a simplified representation of the resulting authenticated image; and,

Fig. 9 illustrates the steps performed in carrying out a second form of the method of the invention.

Corresponding reference characters indicate corresponding parts throughout the drawings.

Best Mode for Carrying Out the Invention

Referring to the drawings, the method of the present invention is used to authenticate a visual image which may be produced in any of a number of different circumstances. For example, a facility F employs a security system 10 to detect the presence of an intruder I who may enter the facility through a door D or window W. The security system employs an imaging means which is represented in Fig. 1 by video cameras V1-V3. The cameras are strategically located throughout the facility to capture an image of an intruder when facility security is breached. In Fig. 2, security system 10 is shown to include a processing means 12 for processing any image captured by a camera V. If it is determined an image from a camera includes that of an intruder, it becomes important to process the image so the intruder's identity can be determined. It is also important that the image be authenticated so if it is stored for later use, or transmitted to the authorities, it can be immediately determined that the image is authentic, or if not, where an alteration to the image has occurred. This is important for evidentiary purposes. Those skilled in the art will recognize other situations in which image authentication is useful. For example, as previously mentioned, it is now common to transmit visual images of a patient from one place to another for diagnostic purposes, for example. Using the method of the present invention, any transmission errors caused for whatever reason, can be immediately ascertained. This prevents the integrity of a transmitted image from being comprised. The method of the present invention provides a unique process by which image authentication is achieved. Further, the encryption techniques employed in

carrying out the process result in the authentication of an image which will be different at one time from another.

Referring to Fig. 3, the original image captured by a camera V comprises a plurality of individual pixels. Each pixel can be converted into a data word, for example, a 6-bit data word. The data words can then arranged into a 2-dimensional formatted array having m rows r and n columns c. A 2-dimensional array of 480 rows and 512 columns is designated A1 in Fig.3. Designations for the pixel locations start at the upper left corner of the array, and proceed across and down the array to the lower right. The value of a pixel in the array at a position m,n is given by $p_{m,n}$ with the upper left pixel in the array being designated $p_{0,0}$, and the pixel in the lower right $p_{479,511}$.

In accordance with the invention, array A1 representing the original image is first converted into a second and, if necessary for data reduction, smaller array A2. In Fig. 4, array A1 is shown to include a plurality of rows r_1, r_2, ...r_{m-1}, r_m, and a plurality of columns c_1, c_2, ... c_{n-1}, c_n. In converting from array A1 to array A2, the process involved may require the elimination of rows and columns from array A1 in accordance with a set of rules. One such set of rules may be:

a) eliminate the even numbered rows if the hour at which the image is formed is an even numbered hour;

b) eliminate the odd numbered rows if the hour at which the image is formed is an odd numbered hour;

c) eliminate the even numbered columns if the day of the month at which the image is formed is an even numbered day; and,

b) eliminate the odd numbered columns if the day of the month at which the image is formed is an odd numbered day.

In accordance with these rules, the resulting array A2 will be a 240x256 2-dimensional array in which the constituent data words included in the array will change from one hour to the next. Further, it will be appreciated that the rules can use other elements for the measure of time (hours and minutes), and also that the rules can require other manipulations beside the elimination of every other row or

column. This means that array A2 could be a larger or smaller array than the 240x256 array shown in Fig. 3.

Once array A1 is converted into array A2, the next step is to convert array A2 into a linear vector A3. This is done by concatenating the data words in the array so they are now arranged linearly as shown in Fig. 5. The first element in linear vector A3 comprises the 6-bit data word for the first pixel $p_{0,0}$ in array A2. The next pixel is $p_{0,1}$, then $p_{0,2}$, and so forth through to pixel $p_{239,255}$. The resulting vector has a vector length of 61,440 data words (240*256).

Linear vector A3 is next transformed into a second linear vector A4. As indicated by the arrows in Fig. 3, the locations of the data words are shuffled so the locations they occupy in array A4 is unique and is determined in accordance with a look-up code provided to processing means 12. According to the code, vector locations in vector A3 are randomly redistributed in vector A4. The position shuffling code is changed on a periodic basis which can be monthly, daily, hourly, or by the minute. As a result, the location of the same words transferred from vector A3 into vector A4 will be different from one time to another.

After forming vector A4, the method next includes the calculation or determination of a checksum for the data words as they are now arranged in this vector. In performing the checksum, a location on the linear vector is selected as a starting location. The location selection is done using a formula which incorporates elements of the time at which the image is formed. Again, these can include the month, day, hour, and minute at which the image is produced, or a combination of the elements. Each of these four time elements may, for example, have a value ascribed to it. The elements are then combined in a predetermined manner. That is, one element may be added to, subtracted from, multiplied with, or divided by another element. Constants can also be used with the elements. Those skilled in the art will appreciate that a wide range of combinations are possible without departing from the scope of the invention. If minutes, for example, are used in the formula, then a starting location determined in

accordance with the formula will change minute by minute. Accordingly, the starting location selected in array A4 at one minute will be different from that which is selected the next minute.

Referring to Fig. 3, the location in array A4 where a checksum determination starts is indicated. As indicated by the Fig., a predetermined block B1 of words, 256 for example, is selected and their corresponding bit values sequentially summed. After the first summation is complete, a second predetermined block B2 is taken and the process repeated. As shown in Fig. 6, the checksum determination includes taking 256 consecutive data words DW1-DW256 from array A4. The most significant bits of each data word are summed together to produce a value Σmsb. The process is repeated for each column of bits until the sum of the least significant bits Σlsb is calculated. Each summation is used to form 6 new data bytes for the respective summation values. Because array A4 includes 240 blocks B1-B240 each having 256 data words, at the end of the checksum process, a sequence of 1,440 bytes (240*6) will have been produced. These bytes now represent an encrypted value of the contents of the original image.

A second checksum is derived by taking the first value previously chosen and adding the bits from the next 256 entries further along (i.e., the first entry in the next block in array A4) and continuing the summation for all 240 blocks of data words. Then starting at the next entry of the original block, another checksum is found. This process is continued until all entries in the block are exhausted, and will result in an additional 256x6 checksum.

Next, a header H is formed using the checksum values and information relating to the camera which produced the image and the time (month, day, hour, and minute) at which the image was formed. As shown in Fig. 7, header H has two parts. The first part HP1 includes the camera and time reference information. The second part HP2 includes the 1440 checksum bytes. It will be understood that the information relating to the camera identification and time reference will comprise a plurality of bytes and the location of these bytes may be scrambled

within header part HP1. It will further be understood that the values for the respective time elements may again be mathematically combined so a month value, for example, may be added, subtracted, multiplied, or divided by a constant value. After the header is formed, it is attached to the initial image array to form a completed authenticated image AI (see Fig. 8). As shown in Fig. 2, this authenticated image is what is supplied by processing means 12 to transmission or storage means 14.

Since header H includes time information about when the image was produced, this information, together with the checksum value can be used to authenticate the image at a later time or different place. If the authentication reveals that the image content is not that of the original image, the location where a change has occurred is determined from by reference to the checksum. Since the formatted image array is a 2-dimensional array, any change in the content will effect values for both the row and column where the change occurs. The checksum value is derived from the information content in the original array, and so incorporates both row and column values. Reference to the checksum will therefore locate where within the array a content value has changed. It will be appreciated that because of all the possible authentication combinations which can result from use of the process, that it is virtually impossible for someone to be able to intentionally change the content value of the image in a way that will not be detected.

Referring to Fig. 9, a second manner for carrying out the method of the invention includes converting the original image array A1 to a second array A2, as before, with the rows and columns which are eliminated being determined in accordance with an established set of rules. Now, instead of converting 2-dimensional array A2 into a linear vector, a third 2-dimensional array A5 is created in which the rows and columns are shuffled in a random sequence. The code by which this shuffling occurs is again periodically changed so that the repositioning which results at one time differs from that which occurs at another. Thus, in array A5, the first pixel no longer is the pixel $p_{0,0}$, but rather a pixel

$p_{mx,ny}$; and the last pixel no longer pixel $p_{239,255}$, but a pixel $p_{ma,nb}$. A checksum is again created, this time by calculating checksums for the rearranged rows and columns in array A5. The location within the array where the checksum determination starts is again based upon a formula which include values representing elements of the time the image is produced. The result is that the location in the array where the checksum starts will be different for one time at which an image formed to another. Once the checksum has been completed, a header H similar to that shown in Fig. 7 is formed. The first portion HP1 of the header again includes location and time information about the image and the second portion HP2 the checksum vector. The header is attached to the original image array A1 to produce the authenticated image AI.

This second way of carrying out the method of the invention also has the advantage of authenticating the image at a later time and also of allowing immediate determination of whether and where a change in content of the original image has occurred. Further, this approach has the advantage of requiring only 496 words (240 + 256) to be processed rather than the 61,440 words required in executing the method as previously described.

What has been described is a method of authenticating visual images to verify that the content of an image viewed at a later time is the same as that when the image was produced. Or, if the image content has changed, this is readily detected as well as the location within the image where a change has occurred. The image is encrypted at its source and the authentication remains with the image regardless of its subsequent use. For this purpose, the algorithm used to produce the authenticated image is incorporated in image processing equipment located at the site where the image is produced and authentication occurs at the time the image is produced. Authentication is accomplished by an algorithm which may include as one factor elements of the time at which the image is formed. These elements includes the month, day, hour, and minute at which the image is created. Because encryption can change on a basis of time, an authentication code for an image at one time will be different from an authentication code for the same

image made at a different time. Also, because of the range of combinations which can possibly be used to authenticate an image it is virtually impossible for a change in image content to go undetected. The method is useful in a wide range of applications where it is image content be must be verified at a different time or place from those where the image is created.

In view of the foregoing, it will be seen that the several objects of the invention are achieved and other advantageous results are obtained.

As various changes could be made in the above constructions without departing from the scope of the invention, it is intended that all matter contained in the above description or shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.

Claims

1. A method of authenticating a video image by forming the image into a data format, encrypting a portion of the formatted image, and attaching the encrypted portion to the original image so the content of the original image can thereafter be authenticated by reference to the encrypted portion thereof.

2. The method of claim 1 further including detecting any modification to the content of the original image and determining where in the image the modification occurred.

3. The method of claim 1 further including forming a header for the formatted image using the encrypted portion thereof, attaching the header to the formatted image, and storing or transmitting the header with the formatted image for authenticating the image.

4. The method of claim 1 wherein the formatted image comprises a 2-dimensional array of pixels each of which is represented by a data word of a defined length and the method includes converting the formatted image from said 2-dimensional array into a second 2-dimensional array.

5. The method of claim 4 wherein forming the second 2-dimensional array includes manipulating the rows and columns of the formatted array by a set of rules which incorporate the time at which the original image is formed.

6. The method of claim 5 further including converting the second 2-dimensional array into a linear vector by concatenating the data words contained in the second array.

7. The method of claim 6 further including converting the aforesaid linear vector into a second linear vector in which the position of the data words in the first linear vector are located at different positions in the second linear vector, the positioning of the data words in the second linear array being determined in accordance with a predetermined code by which the data words are randomly positioned in the second linear vector.

8. The method of claim 7 further including determining a checksum using the data words as arranged in the second linear vector, the checksum

determination beginning at a location in the second linear vector which is established by a formula in which values representing elements of the time at which the image is formed are included.

9. The method of claim 8 wherein determining the checksum includes successively summing the values of each of the bits comprising a predetermined number of data words, the summation beginning with the most significant bit in each data word and proceeding through to the summation of the least significant bit thereof.

10. The method of claim 9 wherein determining the checksum further includes computing a checksum for blocks of data words each of which comprises the predetermined number of data words until a checksum is produced which includes all the data words in the second linear vector.

11. The method of claim 9 further including forming a header which is attached to the formatted array, one portion of the header including data words representing the checksum value for the data words contained in the second linear vector, the checksum value contained in the header being used to authenticate the contents of the formatted image.

12. The method of claim 11 wherein another portion of the header is formed by combining information relating to an identity and location of a device used to form the image, and the time at which the image is formed.

13. The method of claim 3 wherein the operations performed in producing the authentication are incorporated in an algorithm, portions of the algorithm including values representing elements of the time at which the image is formed, the values of the time elements periodically changing whereby an authentication for a formatted image produced at one time would be different from the authentication for the same formatted image if produced at a different time.

14. The method of claim 5 further including repositioning the rows and columns in the second array, the repositioning being determined in accordance with a predetermined code by which the rows and columns are randomly repositioned into a third 2-dimensional array.

15. The method of claim 14 further including determining a checksum for the third array by successively summing the values of the bits forming the data words for each row and column of the third array, the summation beginning by summing all of the most significant bits in the data words and proceeding through to the least significant bits thereof, the checksum determination beginning at a location in the third array established by a formula in which values representing elements of the time at which the image is formed are included.

16. The method of claim 15 further including forming a header which is attached to the formatted array, one portion of the header including data words representing the checksum value for the data word values contained in the third array, the checksum value contained in the header being used to authenticate the contents of the formatted image.

17. The method of claim 16 wherein another portion of the header is formed by combining information relating to an identity and location of a device used to form the image, and the time at which the image is formed.

18. A method of authenticating a video image comprising creating a video image using a video device; formatting the image created by the device into a first 2-dimensional pixel array in which each pixel is represented by a data word of a predetermined length; converting the first 2-dimensional array into a second 2-dimensional array by manipulating the rows and columns in the first array; forming a linear vector using the data words in the second array with the location of data words being randomly selected; determining a checksum from the data words in the linear vector; forming a header using the checksum, information identifying the device used to create the image, and the time at which the image is formed; and, attaching the header to the formatted array representing the original contents of the image for the header to be stored or transmitted with the formatted array with the information contained in the header used to authenticate the image.

19. The method of claim 18 wherein the second array is smaller in size than the first array and is formed by eliminating selected rows and columns in the first array, the rows and columns which are eliminated being determined in accordance

with a set of rules incorporating elements of the time at which the image is formed.

20. The method of claim 19 further including converting the second array into a first linear vector by concatenating the data words in the second array.

21. The method of claim 20 further including converting the first linear vector into a second linear vector in which the position of the data words in the first linear vector are located at different positions in the second linear vector, the positioning of the data words in the second linear array being determined in accordance with a predetermined code by which the data words are randomly positioned in the second linear vector.

22. The method of claim 21 wherein determining the checksum includes selecting a predetermined number of consecutive data words in the second linear vector; summing the contents of the data words beginning by summing all of the most significant bits in the data words and proceeding through to the least significant bits; and, computing a checksum for blocks of data words each of which comprises the predetermined number of data words until a checksum is produced which includes all the data words in the second linear vector, the location in the second linear vector where the checksum determination begins being established by a formula in which values representing elements of the time at which the image is formed are included.

23. The method of claim 22 wherein the location in the second linear vector where the checksum determination begins is a function of the month, day, hour, and minute at which the image is formed.

24. The method of claim 22 wherein forming the header includes forming a first portion of the header by combining together information relating to an identity and location of a device used to form the image, and the time at which the image is formed; and, forming a second portion of the header including the checksum value for all the data words in the second linear vector.

25. A method of authenticating a video image comprising creating a video image using a video device; formatting the video image into a 2-dimensional pixel

array in which each pixel is represented by a data word of a predetermined length; converting the formatted array into a second 2-dimensional array by manipulating the rows and columns forming the formatted array; determining a checksum from the data words forming the second array; forming a header using the checksum, information identifying the device used to create the image, and the time at which the image is formed; and, attaching the header to the formatted array and storing or transmitting the header with the formatted array to authenticate the content of the original image as stored in the formatted array.

26. The method of claim 25 wherein the second array is smaller in size than the formatted array and is formed by eliminating selected rows and columns in the formatted array, the rows and columns which are eliminated being determined in accordance with a set of rules incorporating elements of the time at which the image is formed.

27. The method of claim 26 further including repositioning the rows and columns of the second array into a third 2-dimensional array, the repositioning being determined in accordance with a predetermined code by which the rows and columns are randomly repositioned into the third array.

28. The method of claim 27 wherein determining the checksum for the third array includes successively summing the values of the bits forming the data words for each row and column of the third array, the summation beginning by summing all of the most significant bits in the data words and proceeding through to the least significant bits thereof, the checksum determination beginning at a location in the third array established by a formula in which values representing elements of the time at which the image is formed are included.

29. The method of claim 28 wherein forming the header includes forming a first portion of the header by combining together information relating to an identity and location of a device used to form the image, and the time at which the image is formed; and, forming a second portion of the header including the checksum value for all the data words in the third array.

30. A method of authenticating a video image comprising creating a video image using a video device; formatting the image created by the device into a first 2-dimensional pixel array in which each pixel is represented by a data word of a predetermined length; converting the first 2-dimensional into a second 2-dimensional array which is a smaller array than the first array, the conversion from the first to the second 2-dimensional array being performed by eliminating rows and columns from the first array in accordance with a set of rules incorporating elements of the time at which the image is formed; converting the second array into a linear vector by which the position of the data words is determined in accordance with a predetermined code by which the data words are randomly positioned in the linear vector; determining the checksum for the image by summing the contents of all of the data words in the linear vector beginning at a location established by a formula in which values representing elements of the time at which the image is formed are included; forming a header using the resulting checksum, information identifying the device used to create the image, and the time at which the image is formed, and attaching the header to the formatted array representing the original contents of the image for the header to be stored or transmitted with the formatted array with the information contained in the header used to authenticate the image.

31. A method of authenticating a video image comprising creating a video image using a video device; formatting the video image into a 2-dimensional pixel array in which each pixel is represented by a data word of a predetermined length; converting the formatted array into a second 2-dimensional array by eliminating selected rows and columns in the formatted array, the rows and columns which are eliminated being determined in accordance with a set of rules incorporating elements of the time at which the image is formed; repositioning the rows and columns of the second array into a third 2-dimensional array, the repositioning being determined in accordance with a predetermined code by which the rows and columns are randomly repositioned into the third array; determining a checksum for the image by summing the contents of all of the data words in the third array

beginning at a location established by a formula in which values representing elements of the time at which the image is formed are included; forming a header using the checksum, information identifying the device used to create the image, and the time at which the image is formed; and, attaching the header to the formatted array and storing or transmitting the header with the formatted array to authenticate the content of the original image as stored in the formatted array.

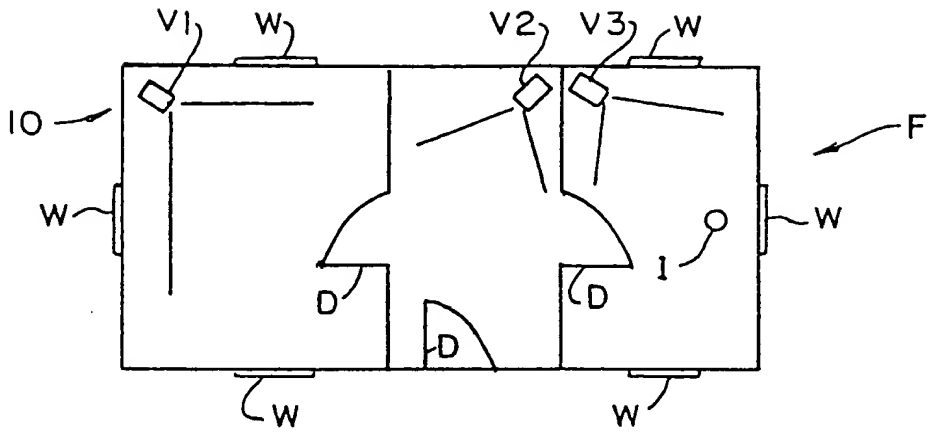


FIG.1

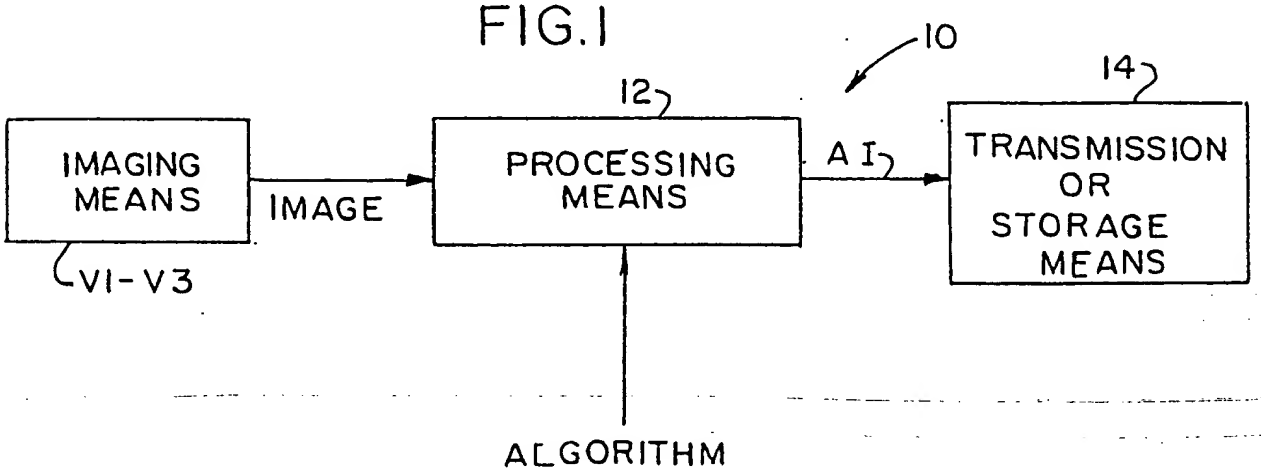


FIG.2

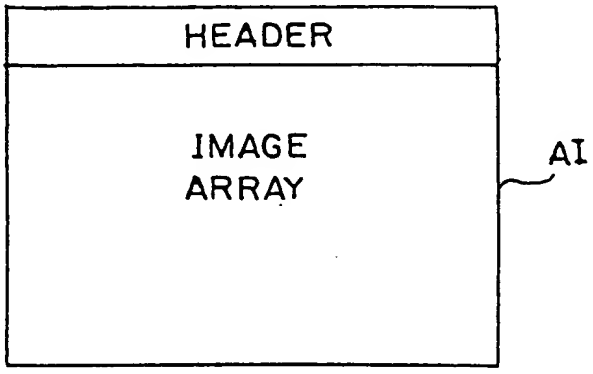


FIG.8

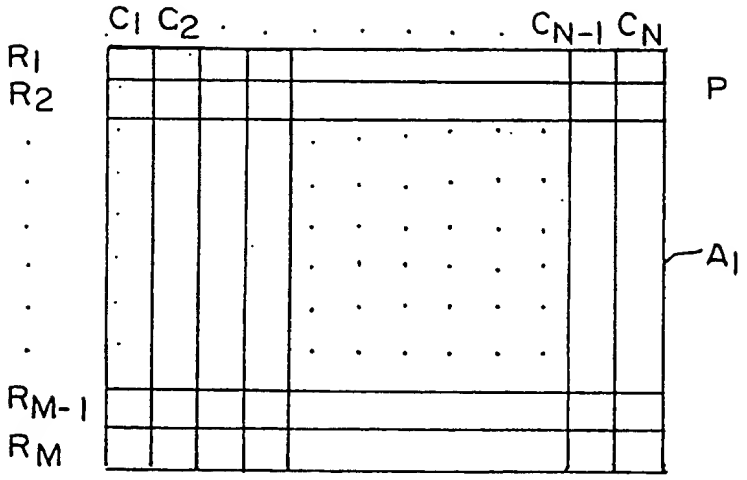


FIG. 4

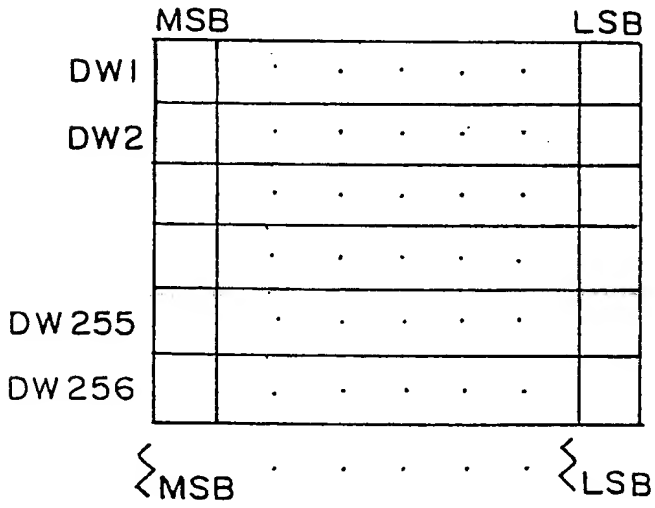


FIG. 6

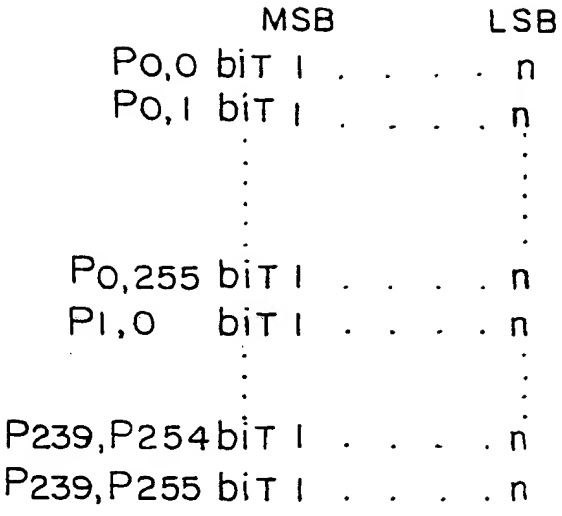


FIG. 5

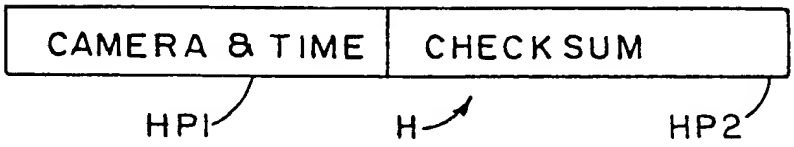


FIG. 7

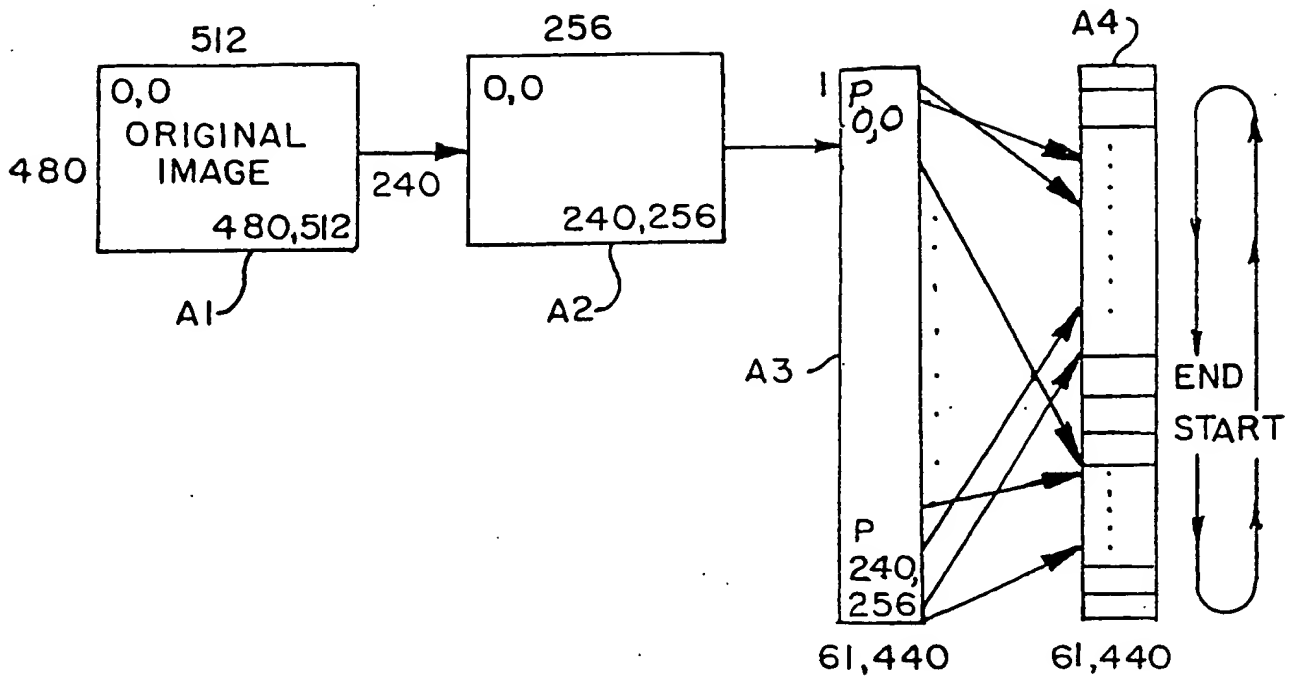

512
0,0
ORIGINAL
IMAGE
480
480,512
240
A1
256
0,0
240,256
A2
1
P
0,0
A3
P
240,
256
61,440
A4
61,440
END
START

FIG. 3

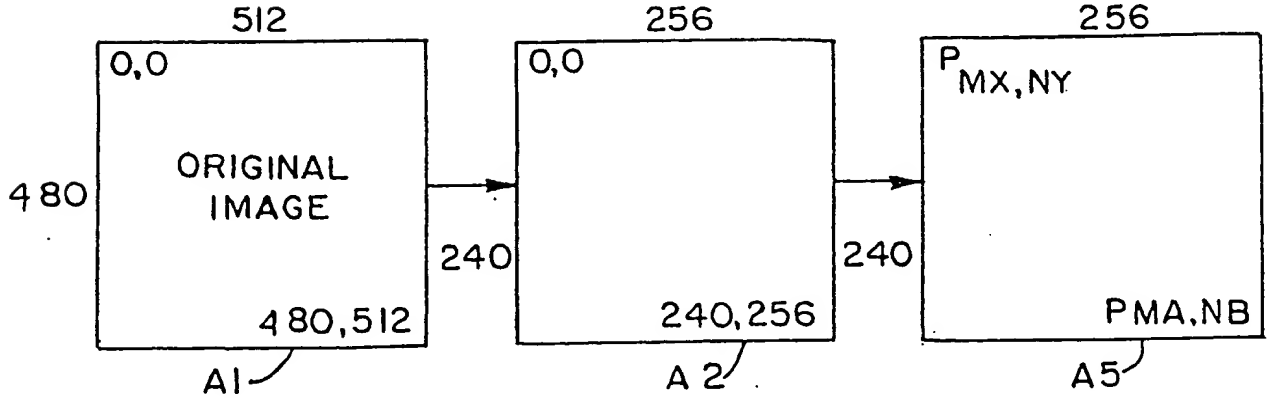

512
0,0
ORIGINAL
IMAGE
480
480,512
240
A1
256
0,0
240,256
A2
240
256
P MX,NY
PMA,NB
A5

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/21789

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/32
US.CL :380/10, 23
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/10, 23; 348/232, 441, 552; 382/253

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS-USPAT: AUTHENTICAT?, IMAGE#, VIDEO, PIXEL, VECTOR, ENCRYPT?

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,499,294 A (FRIEDMAN) 12 MARCH 1996, col. 4, lines 30-46, col.9, lines 8-28.	1-3 and 13
X	US 5,579,393 A (CONNER ET AL) 26 NOVEMBER 1996, col. 5, lines 28-41, col. 6, lines 55-68.	1-3 and 13
A	US 4,972,476 A (NATHANS) 20 NOVEMBER 1990, col. 4, lines 5-24.	18, 25, 30 and 31
A	US 5,231,663 A (EARL ET AL) 27 JULY 1993, col. 1, lines 55-65.	18, 25, 30 and 31

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 04 MARCH 1998	Date of mailing of the international search report 0 8 APR 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GILBERTO BARRÓN JR. Telephone No. (703) 305-1830

Form PCT/ISA/210 (second sheet)(July 1992)*